Random Matrices and the Riemann zeta function

Paul Bourgade[(1)] and Marc Yor[(1),(2)]

(1) Laboratoire de Probabilités et Modèles Aléatoires, Universités Paris VI et VII, 4 Place Jussieu - Case 188, F-75252 Paris Cedex 05
(2) Institut Universitaire de France

Abstract. These notes are based on a talk given at the Institut de Mathématiques Élie Cartan de Nancy in June 2006. Their purpose is to introduce the reader to some links between two fields of mathematics : analytic number theory and random matrices. After some historical overview of these connections, we expose a conjecture about the moments of the Riemann zeta function, formulated by Keating and Snaith in [8]. Last, we give some probabilistic interpretations of their corresponding results about unitary random matrices.

1 Introduction

1.1 The Riemann zeta function : definition and some conjectures

Following Patterson in [10] the Riemann zeta function can be defined, for $\sigma := \Re(s) > 1$, as a Dirichlet series or an Euler product :

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}},$$

where $\mathcal{P}$ is the set of all prime numbers. This function admits a meromorphic continuation to $\mathbb{C}$, and is regular except at the single pole $s = 1$, with residue 1. Moreover, the classical functional equation holds :

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s). \tag{1}$$

The zeta function admits trivial zeros at $s = -2, -4, -6, \dots$ corresponding to the poles of $\Gamma(s/2)$. From equation (1) one can check that all non-trivial zeros are confined to the "critical strip" $0 \leq \sigma \leq 1$, and they are symmetrically positioned about the real axis and the "critical line" $\sigma = 1/2$. The Riemann hypothesis states that all these zeros lie on the critical line.

The importance of the Riemann hypothesis in many mathematical fields justifies the intensive studies which continue to be made about the behavior of $\zeta(1/2 + it)$ for $t \geq 0$. In particular, there is the following famous conjecture, which is implied by the Riemann hypothesis.

The Lindelöf hypothesis. *For every $\varepsilon > 0$, as $t \to \infty$,*

$$\left|\zeta\left(\frac{1}{2}+it\right)\right| = O(t^{\varepsilon}). \tag{2}$$

This conjecture can be shown to be equivalent to another one relative to the moments of ζ on the critical line.

The moments hypothesis. *For all $\varepsilon > 0$ and $k \in \mathbb{N}$, as $T \to \infty$,*

$$I_k(T) := \frac{1}{T}\int_0^T \mathrm{d}s \left|\zeta\left(\frac{1}{2}+is\right)\right|^{2k} = O(T^{\varepsilon}). \tag{3}$$

Equation (3) may be easier to study than (2), because it deals with means of ζ and no values at specific points.

By modeling the zeta function with the characteristic polynomial of a random unitary matrix, Keating and Snaith [8] even got a conjecture for the exact equivalent of $I_k(T)$. This will be exposed in part 3 of these notes, and urges us to define precisely some families of random matrices for compact groups.

1.2 Random matrices : classical compact groups and Haar measure

Let us first define the following classical compact groups :

- $O(n)$ (orthogonal group) is the set of $n \times n$ matrices O such as $OO^T = I_n$;
- $SO(n)$ is the subgroup of $O(n)$ of matrices A with $\det(A) = 1$;
- $U(n)$ (unitary group) is the set of $n \times n$ matrices U such as $UU^* = I_n$, with U^* the conjugate of U^T ;
- $USp(2n)$ (the symplectic group) is the subgroup of $U(2n)$ of matrices U commuting with $\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$.

General theory about topological groups implies the following well-known result.

Existence and uniqueness of a Haar measure. *Let $\Gamma = O(n)$, $SO(n)$, $U(n)$ or $USp(n)$. There exists a unique probability measure μ_Γ on Γ such as :*

- *$\mu_\Gamma(A) > 0$ for all nonempty open sets $A \subset \Gamma$;*
- *$\mu_\Gamma(gA) = \mu_\Gamma(A)$ for all $g \in \Gamma$ and nonempty open sets $A \subset \Gamma$.*

This measure μ_Γ is called the Haar measure of Γ.

There is no generic way to choose an element of a group endowed with the Haar measure, but for the special cases considered here, we mention the following results, with no proofs.

- Let G be a random $n \times n$ matrix, with all G_{jk}'s independent standard normal variables. Then, if O is the Gram-Schmidt transform of G, its distribution is the Haar measure $\mu_{O(n)}$.

  The same method for generating an element of $U(n)$ applies, with this time $G_{jk} = a_{jk} + ib_{jk}$, and all a_{jk}'s and b_{jk}'s standard independent normal variables.
- A decomposition of an orthogonal matrix into reflections leads to the following generator of $\mu_{O(n)}$, as proven in [9].

  Let e_1 be the unit vector corresponding to the first coordinate of $\mathbb{R}^n$, and v be a unit vector chosen uniformly on the sphere $\mathcal{S}_n$. Let

  $$u := \frac{v + e_1}{|v + e_1|}$$

be the unit vector along the bisector of v and e_1 (u is well-defined with probability 1). The reflection with respect to the hyperplane orthogonal to u is $H(v) = I_n - 2uu^T$. If O_{n-1} is distributed with the Haar measure $\mu_{O_{n-1}}$, and v is uniformly distributed on $\mathcal{S}_n$, independently of O_{n-1}, then

$$O_n := H(v) \begin{pmatrix} 1 & 0 \\ 0 & O_{n-1} \end{pmatrix} \tag{4}$$

is distributed with the Haar measure μ_{O_n}. Similar decompositions for $U(n)$ and $USp(2n)$ exist. A decomposition like (4) can be useful to compute the law of some functionals of random matrices.

Let us now consider specially the unitary group $U(n)$. The Haar measure induces a measure on the eigenvalues $(e^{i\theta_1}, \dots, e^{i\theta_n})$ of a unitary matrix. More precisely, the following formula holds.

Weyl's integration formula. *With the previous notations, the joint distribution of* $(\theta_1, \dots, \theta_n)$ *is given by*

$$\mu_{U(n)}(\mathrm{d}\theta_1, \dots, \mathrm{d}\theta_n) = \frac{1}{(2\pi)^n n!} \prod_{1 \le j < m \le n} \left| e^{i\theta_j} - e^{i\theta_m} \right|^2 \mathrm{d}\theta_1 \dots \mathrm{d}\theta_n. \tag{5}$$

Similar formulas exist for other compact groups, but we shall not need them in the following.

2 The zeta function and random unitary matrices : probabilistic links

2.1 The encounter of Montgomery and Dyson

Let us assume the Riemann hypothesis and write all non-trivial roots of the zeta function $1/2 \pm it_n$ with $0 < t_1 \le t_2 \le \dots \le t_n \le \dots$ After making the normalization $w_n = \frac{t_n}{2\pi} \log \frac{t_n}{2\pi}$, it has been shown that

$$\frac{N(W)}{W} \underset{W \to \infty}{\longrightarrow} 1,$$

where $N(W) = |n : w_n < W|$. This is a key step for an analytic proof of the prime number theorem, shown independently by Hadamard and de la Vallée Poussin in 1896. A further step is the study of the pair correlation

$$\frac{1}{W} \left| (w_n, w_m) \in [0, W]^2 : \ \alpha \le w_n - w_m \le \beta \right|,$$

and more generally the operator

$$R_2(f, W) = \frac{1}{W} \sum_{1 \le j,k \le N(W), j \ne k} f(w_j - w_k).$$

The following theorem establishes the asymptotics of $R_2(f, W)$ for a large class of functions f.

Theorem (Montgomery, 1973). *If the Fourier transform of* f *(*$\hat{f}(\tau) := \int_{-\infty}^{\infty} \mathrm{d}x f(x) e^{2i\pi x\tau}$*) has a compact support included in* $[-1, 1]$*, then*

$$R_2(f, W) \underset{W \to \infty}{\longrightarrow} \int_{-\infty}^{\infty} \mathrm{d}x f(x) R_2(x) \tag{6}$$

with

$$R_2(x) := 1 - \left(\frac{\sin \pi x}{\pi x} \right)^2.$$

A conjecture due to the number theorist H. L. Montgomery states that the result remains true even if $\hat{f}$ has no compact support, and this problem is still open…

Is there a connection with Random Matrix Theory ? In 1972, at the Princeton Institute for Advanced Studies, Montgomery and some colleagues stopped working for afternoon tea, an important ritual for most mathematics departments. There, he was introduced to the quantum physicist Freeman Dyson by Indian number theorist Daman Chowla. Then Montgomery described his model for the pair correlation of zeros of the zeta function, and Dyson recognized the pair correlation of eigenvalues of a unitary matrix... The connection was born !

More precisely, let $(e^{i\theta_1}, \dots, e^{i\theta_N})$ be the eigenvalues of an element $A \in U(N)$. We write

$$\phi_n := \frac{N}{2\pi}\theta_n$$

for the normalized angles (θ_n is considered modulo 2π, but not ϕ_n). Then it can be shown that

$$\frac{1}{N}\int_{U(N)} \mathrm{d}\mu_{U(N)}(A)\,|(n,m)\ :\ \alpha < \phi_n - \phi_m < \beta| \underset{N\to\infty}{\longrightarrow} \int_\alpha^\beta \mathrm{d}x \left(1 - \left(\frac{\sin \pi x}{\pi x}\right)^2\right),$$

and, more generally, for a continue function f with compact support, the asymptotic law of the pair correlation for eigenvalues in $U(N)$ is given by

$$\frac{1}{N}\int_{U(N)} \sum_{j\neq k} f(\phi_j - \phi_k)\mathrm{d}\mu_{U(N)}(A) \underset{N\to\infty}{\longrightarrow} \int_{-\infty}^{\infty} \mathrm{d}x f(x) R_2(x). \tag{7}$$

The similarity between formulas (6) and (7) suggests a strong connection between the zeros of the Riemann zeta function and the spectra of the random unitary matrices.

This link is reinforced by the Polya-Hilbert program : if one writes the non trivial zeros of the zeta function as $1/2 \pm it_n$ $(n \geq 1)$, showing that the t_n's are the eigenvalues of an hermitian operator would imply the Riemann hypothesis.

2.2 Two central limit theorems

The law of a unitary matrix determinant gives another example of similarity between Random Matrix Theory and the zeta function.

First, we recall the following famous result due to Selberg.

Theorem. *For any regular*[1] *Borel set* $\Gamma \subset \mathbb{C}$

$$\frac{1}{T}\int_T^{2T} \mathrm{d}t \mathbb{1}\left(\frac{\log\zeta\left(\frac{1}{2}+it\right)}{\sqrt{\frac{1}{2}\log\log T}} \in \Gamma\right) \underset{T\to\infty}{\longrightarrow} \iint_\Gamma \frac{\mathrm{d}x\mathrm{d}y}{2\pi} e^{-\frac{x^2+y^2}{2}} \tag{8}$$

(here, and in the following, log is a continuous determination of the complex logarithm).

In other terms, if our probability space is the interval $[1,2]$, fitted with Lebesgue measure $(\mathrm{d}u)$, and if

$$L_T(u) := \frac{\log\zeta\left(\frac{1}{2}+iuT\right)}{\sqrt{\frac{1}{2}\log\log T}},$$

then, with $\mathcal{N}$ standing for a standard normal variable on $\mathbb{C}$,

$$L_T \underset{T\to\infty}{\overset{\text{law}}{\longrightarrow}} \mathcal{N}.$$

[1] Here, regular means that its boundary has zero Lebesgue measure.

This theorem admits a "cousin", concerning the characteristic polynomial of a generic unitary matrix $A \in U(N)$. Precisely, let us define

$$Z(A,\theta) := \det\left(I_N - Ae^{-i\theta}\right) = \prod_{n=1}^{N}\left(1 - e^{i(\theta_n - \theta)}\right), \tag{9}$$

where $e^{i\theta_1}, \dots, e^{i\theta_N}$ are the eigenvalues of A.

Theorem. *For any regular Borel set* $\Gamma \subset \mathbb{C}$

$$\int_{U(N)} \mathrm{d}\mu_{U(N)}(A) \mathbb{1}\left(\frac{\log Z(A,\theta)}{\sqrt{\frac{1}{2}\log N}} \in \Gamma\right) \underset{N\to\infty}{\longrightarrow} \iint_{\Gamma} \frac{\mathrm{d}x\mathrm{d}y}{2\pi} e^{-\frac{x^2+y^2}{2}} \tag{10}$$

Note that the limit does not depend on θ : by definition, the Haar measure is invariant under action of the unitary group (especially under action of $e^{i\theta} I_N$), so the law of $Z(A,\theta)$ is the same as the law of $Z(A,0)$.

Remark 1 : about the interval $[T, 2T]$ in Selberg's theorem. One may ask what happens if instead of integrating between T and $2T$ one does so on the interval $[0,T]$. A simple dominated convergence argument shows that there is no difference in doing so. Here is the argument. Denote

$$\gamma(t,T) := \mathbb{1}\left(\frac{\log\zeta\left(\frac{1}{2}+it\right)}{\sqrt{\frac{1}{2}\log\log T}} \in \Gamma\right).$$

Then, write

$$\frac{1}{T}\int_0^T \mathrm{d}t\ \gamma(t,T) = \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \underbrace{\frac{1}{2^{-(n+1)}T}\int_{2^{-(n+1)}T}^{2^{-n}T} \mathrm{d}t\ \gamma(t,T)}_{=:u_n(T)}.$$

As $\log\log(2^{-(n+1)}T) \underset{T\to\infty}{\sim} \log\log T$, every $u_n(T)$ converges to $\iint_\Gamma \frac{\mathrm{d}x\mathrm{d}y}{2\pi} e^{-\frac{x^2+y^2}{2}}$. Moreover, the $u_n(T)$'s are uniformly bounded (by $\sup_{T>0} \frac{1}{T}\int_T^{2T} \mathrm{d}t\ \gamma(t,T) < \infty$) as $T \to \infty$, so from the dominated convergence argument one can exchange the sum and the limit, which gives the result.

Remark 2 : a "true" multidimensional generalization of Selberg's theorem. In order to transform the "static" limit in law (8) into a "dynamic" one (ie : showing the convergence in law of a sequence of processes towards another process), it is somewhat natural to replace T by N^λ with $\lambda > 0$.

For a fixed λ, we define

$$\mathcal{L}_\lambda(u,N) := \frac{\log\zeta\left(\frac{1}{2}+iuN^\lambda\right)}{\sqrt{\frac{1}{2}\log N}}.$$

Then, if u is uniformly distributed on $[1,2]$, Selberg's theorem immediately implies that

$$\mathcal{L}_\lambda(\bullet, N) \underset{N\to\infty}{\overset{\text{law}}{\longrightarrow}} \mathcal{N}_\lambda,$$

where

$$\mathbb{P}(\mathcal{N}_\lambda \in \mathrm{d}x\mathrm{d}y) = \frac{1}{2\pi\lambda} e^{-\frac{x^2+y^2}{2\lambda}} \mathrm{d}x\mathrm{d}y. \tag{11}$$

As λ varies, there is the following multidimensional extension of (8) and (11).

Theorem. *([7]) For $0 < \lambda_1 < \lambda_2 < \cdots < \lambda_k$,*

$$\int_1^2 \mathrm{d}y \; \mathbb{1}\left(\mathcal{L}_{\lambda_1}(u,N) \in \Gamma_1, \ldots, \mathcal{L}_{\lambda_k}(u,N) \in \Gamma_k\right) \underset{N\to\infty}{\longrightarrow} \prod_{i=1}^{k} \mathbb{P}(\mathcal{N}_{\lambda_i} \in \Gamma_i),$$

a result which may be interpreted as the convergence of the finite dimensional marginals of $\{\mathcal{L}_\lambda(\bullet, N), \lambda > 0\}$ towards those of $\{\mathcal{N}_\lambda, \lambda > 0\}$, which denotes the totally disordered Gaussian process : its components are all independent, $\mathcal{N}_\lambda$ being distributed as indicated in (11).

This theorem suggests some comments.

- The process $(\mathcal{N}_\lambda, \lambda > 0)$ does not admit a measurable version. Assuming the contrary we would obtain by Fubini : for every $a < b$, $\int_a^b \mathrm{d}\lambda \; \mathcal{N}_\lambda = 0$. Thus $\mathcal{N}_\lambda = 0$, $\mathrm{d}\lambda$ a. s., which is absurd.
- In the asymptotic study of the occupation measure of planar Brownian motion $(Z_t, t \geq 0)$, where for $f \in L^1(\mathbb{C}, \mathrm{d}x\mathrm{d}y)$ there is the convergence in law of $\frac{1}{\log T}\int_0^T \mathrm{d}t f(Z_t)$ towards an exponential variable, the change of scale $T = N^\lambda$ was also performed, but the resulting limiting process $(\overline{f} \cdot e_\lambda, \lambda > 0)$ is not totally disordered but is in fact an "honest" measurable process.
- A totally disordered Gaussian process $(X(\theta) + iY(\theta))$ has also been encountered by Hugues, Keating and O'Connell in [6]. They have proven that, with the notation (9),

  $$\frac{\log Z_N(A,\theta)}{\sqrt{\frac{1}{2}\log N}}$$

  converges weakly towards a totally disordered process with covariance

  $$\mathbb{E}\left(X(\theta_1)X(\theta_2)\right) = \mathbb{E}\left(Y(\theta_1)Y(\theta_2)\right) = \delta(\theta_1 - \theta_2).$$

3 The Keating-Snaith conjecture

3.1 The moments of zeta

In the following we keep the notation from (3) for the moments of the zeta function. The mean $I_k(T)$ has been extensively studied, but its equivalent is well known in only two cases :

– $I_1(T) \underset{T\to\infty}{\sim} \log T$ (Hardy-Littlewood, 1918) ;

– $I_2(T) \underset{T\to\infty}{\sim} \frac{1}{2\pi T}(\log T)^2$ (Ingham, 1926).

Keating and Snaith [8] have formulated the following conjecture about the asymptotics of $I_k(T)$.

The Keating-Snaith conjecture. *For every $k \in \mathbb{N}^*$*

$$I_k(T) \underset{T\to\infty}{\sim} H_{Mat}(k) H_{\mathcal{P}}(k) (\log T)^{k^2}$$

with the following notations :

- *the "arithmetic" factor*

$$H_{\mathcal{P}}(k) := \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p}\right)^{k^2} \left(\sum_{m=0}^{\infty} \left(\frac{\Gamma(k+m)}{m!\Gamma(k)}\right)^2 \frac{1}{p^m}\right);$$

- *the "matrix" factor*

$$H_{Mat}(k) := \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}. \qquad (12)$$

Here are some first steps to understand the origins of this conjecture.

- Imagine that all prime numbers were "independent", in such a way that one might approximate $I_k(T) = \mathbb{E}(|\zeta(s)|^{2k}) = \mathbb{E}\left(\prod_{p\in\mathcal{P}}\left|\frac{1}{1-p^{-s}}\right|^{2k}\right)$ by $\prod_{p\in\mathcal{P}}\mathbb{E}\left(\left|\frac{1}{1-p^{-s}}\right|^{2k}\right)$ (the expectations are taken with respect to Lebesgue measure $\mathrm{d}s/T$ on the segment $[1/2, 1/2+iT]$). Then one would get exactly $H_{\mathcal{P}}(k)(\log T)^{k^2}$ for the equivalent of $I_k(T)$.
  So the coefficient $H_{Mat}(k)$ appears as a constant correction compared to this "independent" model.
- Another model used to approximate the zeta function is the determinant of a unitary matrix : all previous analogies can comfort us in the accuracy of such an approximation. Thanks to Selberg's integral formula [1], Keating and Snaith [8] have calculated the generating function for the determinant of a random unitary matrix with respect to the Haar measure :

$$P_N(s,t) := \mathbb{E}\left(|Z_N(A,\theta)|^t e^{is\arg Z_N(A,\theta)}\right) = \prod_{j=1}^{N}\frac{\Gamma(j)\Gamma(t+j)}{\Gamma(j+\frac{t+s}{2})\Gamma(j+\frac{t-s}{2})}. \tag{13}$$

  Thanks to this closed form, they showed in particular that

$$\mathbb{E}\left(|Z_N(A,\theta)|^{2k}\right) \underset{N\to\infty}{\sim} H_{Mat}(k)N^{k^2},$$

  where $H_{Mat}(k)$ is defined by (12). This led them to introduce this "matrix" factor in the conjectured asymptotic of $I_k(T)$.

However, these two explanations are not sufficient to understand really how these "arithmetic" and "matrix" factors must be combined to get the Keating-Snaith conjecture. A better comprehension of this point is the purpose of the following paragraph.

3.2 Understanding the conjecture : the hybrid GHK model

In [4], Gonek, Hughes and Keating were able to give a partial justification for the Keating-Snaith conjecture based on a particular factorization of the zeta function. More precisely, let us first introduce some notations.

Let $s = \sigma + it$ with $\sigma \geq 0$ and $|t| \geq 2$, let $X \geq 2$ be a real parameter, and let K be any fixed positive integer. Let $u(x)$ be a nonnegative $\mathscr{C}^\infty$ function of mass 1, supported on $[e^{1-1/X}, e]$, and set $U(z) := \int_0^\infty u(x)E_1(z\log x)\mathrm{d}x$, where $E_1(z)$ is the exponential integral $\int_z^\infty (e^{-w}/w)\ \mathrm{d}w$.

Let also

$$P_X(s) := \exp\left(\sum_{n\leq X}\frac{\Lambda(n)}{n^s\log n}\right)$$

where Λ is Van Mangoldt's function ($\Lambda(n) = \log p$ if n is an integral power of a prime p, 0 otherwise), and

$$Z_X(s) := \exp\left(-\sum_{\rho_n} U\left((s-\rho_n)\log X\right)\right)$$

where $(\rho_n, n \geq 0)$ are the imaginary parts of the zeros of ζ. Then the following result, independent of any conjecture, was proved in [4].

Theorem. *With the previous notations,*

$$\zeta(s) = P_X(s)Z_X(s)\left(1 + O\left(\frac{X^{K+2}}{(|s|\log X)^K}\right) + O\left(X^{-\sigma}\log X\right)\right),$$

where the constants before the O only depend on the function u and K.

With this decomposition, the P_X term leads to the "arithmetic" factor of the Keating-Snaith conjecture, while the Z_X term leads to the "matrix" factor. More precisely, this decomposition suggests a proof for the Keating-Snaith conjecture along the following steps.

- First, for a value of the parameter X chosen such as $X = O(\log(T)^{2-\varepsilon})$ here and in the sequel, the following conjecture A suggests that the moments of zeta are well approximated by the product of the moments of P_X and Z_X (they are sufficiently "independent").

  Conjecture A : the splitting hypothesis. *With the previous notations*

$$\frac{1}{T}\int_0^T \mathrm{d}s \left|\zeta\left(\frac{1}{2}+is\right)\right|^{2k} \underset{T\to\infty}{\sim} \left(\frac{1}{T}\int_0^T \mathrm{d}s \left|P_X\left(\frac{1}{2}+is\right)\right|^{2k}\right)\left(\frac{1}{T}\int_0^T \mathrm{d}s \left|Z_X\left(\frac{1}{2}+is\right)\right|^{2k}\right)$$

- Assuming that conjecture A is true, we then need to approximate the moments of P_X and Z_X. The moments of P_X were evaluated in [4], where the following result is proven.

  Theorem : the moments of $\boldsymbol{P_X}$. *With the previous notations,*

$$\frac{1}{T}\int_0^T \mathrm{d}s \left|P_X\left(\frac{1}{2}+is\right)\right|^{2k} = H_{\mathcal{P}}(k)\ \left(e^{\gamma}\log X\right)^{k^2}\left(1+O\left(\frac{1}{\log X}\right)\right).$$

- Finally, a conjecture about the moments of Z_X, if proven, would be the last step.

  Conjecture B : the moments of $\boldsymbol{Z_X}$. *With the previous notations,*

$$\frac{1}{T}\int_0^T \mathrm{d}s \left|Z_X\left(\frac{1}{2}+is\right)\right|^{2k} \underset{t\to\infty}{\sim} H_{Mat}(k)\ \left(\frac{\log T}{e^{\gamma}\log X}\right)^{k^2}.$$

  The reasoning which leads to conjecture B is the following. First of all, the function Z_X is not as complicated as it seems, because as X tends to ∞, the function u tends to the Dirac measure at point e, so

$$Z_X\left(\frac{1}{2}+it\right) \approx \prod_{\rho_n}\left(i(t-\rho_n)e^{\gamma}\log X\right).$$

  The ordinates ρ_n (where ζ is zero) are supposed to have many statistical properties identical to those of the eigenangles of a random element of $U(N)$. In order to make an adequate choice for N, we recall that the γ_n are spaced $2\pi/\log T$ on average, whereas the eigenangles have average spacing $2\pi/N$: thus N should be chosen to be the greatest integer less than or equal to $\log T$. Then the calculation for the moments of this model leads to conjecture B.

4 Probabilistic interpretations for some Keating-Snaith formulas

The main point of this section is to give a simple representation for $Z_N(A,\theta)$, thanks to formula (13). We first recall some results about gamma and beta variables.

4.1 Some formulas about the beta-gamma algebra

A gamma random variable γ_a with coefficient $a > 0$ has density on $[0,\infty[$ given by

$$\frac{\mathbb{P}\left(\gamma_a \in \mathrm{d}t\right)}{\mathrm{d}t} = \frac{t^{a-1}}{\Gamma(a)}e^{-t}.$$

Its Mellin transform is ($s > 0$)

$$\mathbb{E}\left(\gamma_a^s\right) = \frac{\Gamma(a+s)}{\Gamma(a)}. \tag{14}$$

A beta random variable $\beta_{a,b}$ with strictly positive coefficients a and b has density on $[0,1]$ given by

$$\frac{\mathbb{P}\left(\beta_{a,b} \in \mathrm{d}t\right)}{\mathrm{d}t} = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}\, t^{a-1}(1-t)^{b-1}.$$

Its Mellin transform is ($s > 0$)

$$\mathbb{E}\left(\beta_{a,b}^s\right) = \frac{\Gamma(a+s)}{\Gamma(a)}\frac{\Gamma(a+b)}{\Gamma(a+b+s)}.$$

These formulas will also be useful in the following (for justifications, the reader could see [3]).

- The algebra property, where all variables are independent :

$$\beta_{a,b}\gamma_{a+b} \overset{\text{law}}{=} \gamma_a. \tag{15}$$

- The duplication formula for the gamma function, with all variables independent :

$$\gamma_j \overset{\text{law}}{=} 2\sqrt{\gamma_{\frac{j}{2}}\gamma'_{\frac{j+1}{2}}}. \tag{16}$$

4.2 Decomposition of Z_N into independent random variables

Let us recall formula (13) :

$$P_N(s,t) := \mathbb{E}\left(|Z_N(A,\theta)|^t e^{is\arg Z_N(A,\theta)}\right) = \prod_{j=1}^N \frac{\Gamma(j)\Gamma(t+j)}{\Gamma(j+\frac{t+s}{2})\Gamma(j+\frac{t-s}{2})}.$$

Remark. As we already mentioned, the result does not depend on θ, which is a consequence of the definition of the Haar measure. So in the following we will write $\mathbb{E}(f(Z_N))$ for $\mathbb{E}(f(Z_N(A,\theta)))$.

Moreover, this Mellin-Fourier transform implies $\mathbb{E}(Z_N^t) = 1$ for all $t > 0$. A somewhat similar, but more trivial identity is

$$\mathbb{E}\left(e^{s(\mathcal{N}+i\mathcal{N}')}\right) \equiv 1,$$

where $\mathcal{N}$ and $\mathcal{N}'$ are independent, standard, real Gaussian variables : one can show it directly with the independence of $\mathcal{N}$ and $\mathcal{N}'$, or using the fact that $e^{\alpha Z_t}$ is a martingale, with $(Z_t, t \geq 0)$ a complex planar Brownian motion. There does not seem to be a trivial explanation for $\mathbb{E}(Z_N^t) = 1$, but one can give another proof of this result.

Let g be a function on the unitary group $U(N)$, stable on the conjugation classes : $g(U)$ can be written $g(\theta_1,\dots,\theta_N)$, where the $\theta_i' s$ are the eigenangles of U. Then Weyl's formula (5) gives the existence of a density function f invariant by translation ($f(\theta_1,\dots,\theta_N) = f(\theta_1+\theta,\dots,\theta_n+\theta)$) such as

$$\mathbb{E}(g(U)) = \int_{[0,2\pi]^N} g(\theta_1,\dots,\theta_N) f(\theta_1,\dots,\theta_N)\,\mathrm{d}\theta_1\dots\mathrm{d}\theta_N,$$

where the expectation is with respect to the Haar measure.

For the function $g : U \mapsto \det\left((I_N - U)^t\right) = \prod_{k=1}^N \left(1 - e^{i\theta_k}\right)^t$, we get

$$\begin{aligned}
\mathbb{E}\left(Z_N^t\right) &= \int_{[0,2\pi]^N} f(\theta_1, \dots, \theta_N)\ \mathrm{d}\theta_1 \dots \mathrm{d}\theta_N \prod_{k=1}^N \left(1 - e^{i\theta_k}\right)^t \\
&= \int_{[0,2\pi]} \frac{\mathrm{d}\theta}{2\pi} \int_{[0,2\pi]^N} f(\theta_1, \dots, \theta_N)\ \mathrm{d}\theta_1 \dots \mathrm{d}\theta_N \prod_{k=1}^N \left(1 - e^{i\theta_k}\right)^t \\
&= \int_{[0,2\pi]} \frac{\mathrm{d}\theta}{2\pi} \int_{[0,2\pi]^N} f\left(\tilde{\theta}_1 + \theta, \dots, \tilde{\theta}_N + \theta\right)\ \mathrm{d}\tilde{\theta}_1 \dots \mathrm{d}\tilde{\theta}_N \prod_{k=1}^N \left(1 - e^{i(\tilde{\theta}_k + \theta)}\right)^t \\
\mathbb{E}\left(Z_N^t\right) &= \int_{[0,2\pi]^N} f(\tilde{\theta}_1, \dots, \tilde{\theta}_N)\ \mathrm{d}\tilde{\theta}_1 \dots \mathrm{d}\tilde{\theta}_N \underbrace{\int_{[0,2\pi]} \frac{\mathrm{d}\theta}{2\pi} \prod_{k=1}^N \left(1 - e^{i(\tilde{\theta}_k + \theta)}\right)^t}_{(*)}.
\end{aligned}$$

When t is an integer, $(*)$ can be expanded with Newton's binomial formula, and we get $(*) = \int_{[0,2\pi]} \frac{\mathrm{d}\theta}{2\pi} \left(1 + \sum_{l=1}^{Nt} a_l e^{il\theta}\right) = 1$, so $\mathbb{E}(Z_N^t) = 1$. This reasoning can be generalized to the case $t > 0$, but we need to use the definition $u^t = e^{t \log u}$, with exp and log defined by their Taylor series ; the justification of the exchange between integral and sum then becomes tricky.

We now come back to the general Mellin-Fourier transform. It implies the following proposition.

Proposition. *The modulus $|Z_N|$ of the characteristic polynomial Z_N satisfies both identities in law*

$$\prod_{j=1}^N \gamma_j \overset{law}{=} |Z_N| \prod_{j=1}^N \sqrt{\gamma_j \gamma_j'}, \tag{17}$$

$$|Z_N| \overset{law}{=} 2^N \left(\prod_{j=1}^N \sqrt{\beta_{\frac{j}{2},\frac{j}{2}}}\right) \left(\prod_{j=1}^N \sqrt{\beta_{\frac{j+1}{2},\frac{j-1}{2}}}\right), \tag{18}$$

where all random variables are independent and we make the convention $\beta_{a,0} = 1$.

Proof. First, formula (13) with $s = 0$ can be written, for all $t > 0$,

$$\prod_{j=1}^N \frac{\Gamma(j+t)}{\Gamma(j)} = \mathbb{E}\left(|Z_N|^t\right) \prod_{j=1}^N \left(\frac{\Gamma\left(j + \frac{t}{2}\right)}{\Gamma(j)}\right)^2,$$

which translates (thanks to formula (14)) as

$$\prod_{j=1}^N \gamma_j \overset{\text{law}}{=} |Z_N| \prod_{j=1}^N \sqrt{\gamma_j \gamma_j'},$$

because the Mellin transform is injective. To deduce (18) from (17), we successively use formulas (16) and (15) :

$$\gamma_j \overset{\text{law}}{=} 2\sqrt{\gamma_{\frac{j}{2}} \gamma'_{\frac{j+1}{2}}} \overset{\text{law}}{=} 2\sqrt{\left(\beta_{\frac{j}{2},\frac{j}{2}} \gamma_j\right)\left(\beta_{\frac{j+1}{2},\frac{j-1}{2}} \gamma_j'\right)},$$

which gives the desired result. □

As a nice consequence of (17), we show how to recover partially the central limit theorem (10).

Corollary. *The following central limit theorem holds :*

$$\frac{\log |Z_N|}{\sqrt{\frac{1}{2}\log N}} \xrightarrow{\text{law}} \mathcal{N}$$

as N tends to ∞, with $\mathcal{N}$ a standard normal variable.

Proof. Take logarithms on both sides of (17), and subtract expectations :

$$\mathcal{L}_N \stackrel{\text{law}}{=} \log |Z_N| + \frac{1}{2}\left(\mathcal{L}_N + \mathcal{L}'_N\right),$$

with obvious notations. After division by $\sqrt{\frac{1}{2}\log N}$ the LHS converges in law towards $\mathcal{N}(0, 2/3)$. The result follows easily. □

We gave a probabilistic interpretation for the law of $|Z_N|$, but we can do more with the joint law of $(\Re \log Z_N, \Im \log Z_N)$. Indeed, thanks to the Mellin-Fourier transform (13), after some calculation one can check that

$$(\Re \log Z_N, \Im \log Z_N) \stackrel{\text{law}}{=} \left(\prod_{j=1}^{N} \beta_{j,j-1} 2\cos W_j, \sum_{j=1}^{N} W_j\right)$$

with all β's and W's independent, and W_j with density on $[-\pi/2, \pi/2]$

$$\frac{\mathbb{P}(W_j \in \mathrm{d}x)}{\mathrm{d}x} = c_j \cos(x)^j,$$

where c_j is the normalization constant ($c_j = \Gamma(1 + j/2)^2/\Gamma(1 + j)$). Another way to express this result is the following proposition.

Proposition. *There is the representation*

$$Z_N \stackrel{law}{=} \prod_{j=1}^{N} \beta_{j,j-1}(1 - e^{i\tilde{W}_j}) \tag{19}$$

where the beta and $\tilde{W}$ variables are independent. Furthermore, $\tilde{W}_j$ is distributed on $[0, 2\pi]$ as

$$\mathbb{P}(\tilde{W}_j \in \mathrm{d}w) = \frac{c_{2(j-1)}}{2}\left(2\sin\frac{w}{2}\right)^{2(j-1)} \mathrm{d}w.$$

4.3 Mellin type limit theorems

This paragraph shows how the Mellin-Fourier transform (13) implies the central limit theorem (10) and a generalization.

Let us first recall some results about the Barnes' G-function.

- It is defined on the half plane $\Re(1 + z) > 0$ by

$$G(1 + z) := (2\pi)^{\frac{z}{2}} e^{-\frac{(1+\gamma)z^2+z}{2}} \prod_{n=1}^{\infty}\left(1 + \frac{z}{n}\right)^n e^{-z+\frac{z^2}{2n}},$$

where γ is Euler's constant. Its logarithm can be written

$$\log G(1 + z) = (\log 2\pi - 1)\frac{z}{2} - (1 + \gamma)\frac{z^2}{2} + \sum_{n=3}^{\infty}(-1)^{n-1}\zeta(n - 1)\frac{z^n}{n}. \tag{20}$$

- As mentioned by Jacod in [5], the Barnes' G-function appears naturally in some limit theorems. In particular, let $\psi := \Gamma'/\Gamma$ denote the usual dilogarithm function and $\Gamma_N(\lambda) := \mathbb{E}\left(\left(\prod_{j=1}^N \gamma_j\right)^\lambda\right) = \prod_{j=1}^N \frac{\Gamma(j+\lambda)}{\Gamma(j)}$. Then

$$\frac{\Gamma_N(\lambda)}{N^{\frac{\lambda^2}{2}}} e^{-\lambda \sum_{j=1}^N \psi(j)} \underset{N\to\infty}{\longrightarrow} \frac{\left(\frac{2\pi}{e}\right)^{\frac{\lambda}{2}}}{G(1+\lambda)}. \tag{21}$$

Keating and Snaith [8] are able to recover (10) after writing the series expansion of $P_N(s,t)$. For simplicity, let us consider the case $s=0$. Then one can write

$$P_N(0,t) = \mathbb{E}(|Z_N|^t) = \exp\left(\sum_{m=0}^\infty \alpha_m^{(N)} \frac{t^m}{m!}\right),$$

that is : the coefficients $\alpha_m^{(N)}$ $(m = 0,1,\dots)$ are the cumulants of $\log|Z_N|$. From (13), one obtains

$$\left\{\begin{array}{lcl} \alpha_0^{(N)} & = & \alpha_1^{(N)} = 0 \\ \alpha_2^{(N)} & = & \frac{1}{2}\log N + \frac{1}{2}(\gamma+1) + O\left(\frac{1}{N^2}\right) \\ \alpha_m^{(N)} & = & (-1)^m\left(1-\frac{1}{2^{m-1}}\right)\Gamma(m)\zeta(m-1) + O\left(\frac{1}{N^{m-2}}\right),\ m\geq 3 \end{array}\right. . \tag{22}$$

Thus, it follows that

$$\mathbb{E}\left(\exp\left(t\frac{\log|Z_N|}{\sqrt{\frac{1}{2}\log N}}\right)\right) = \mathbb{E}\left(|Z_N|^{\frac{t}{\sqrt{\frac{1}{2}\log N}}}\right) \underset{N\to\infty}{\longrightarrow} e^{\frac{t^2}{2}},$$

which yields to the central limit theorem for $\log|Z_N|$. However, the previous analysis shows more than (10) : from the expression (22) of the cumulants and formula (20), Keating and Snaith immediately get the following theorem.

Mellin-type limit theorem. *For* $|\lambda| < 1/2$,

$$\frac{1}{N^{\lambda^2}}\mathbb{E}\left(|Z_N|^{2\lambda}\right) \underset{N\to\infty}{\longrightarrow} \frac{G(1+\lambda)^2}{G(1+2\lambda)}.$$

Remark. Rather than using directly the information about the cumulants given in (22), one can show the previous theorem with the duplication identity (17) and the limit (21).

Moreover, one can write (13) as

$$P_N(s,t) = \frac{\Gamma_N(t)}{\Gamma_N\left(\frac{t+s}{2}\right)\Gamma_N\left(\frac{t-s}{2}\right)},$$

with the notations of (21). Then, using the limit (21), we get the following generalization of the Mellin-type limit theorem.

Proposition. *If* $t \geq |s|$,

$$\frac{1}{N^{\frac{t^2-s^2}{4}}} P_N(s,t) \underset{N\to\infty}{\longrightarrow} \frac{G\left(1+\frac{t+s}{2}\right)\ G\left(1+\frac{t-s}{2}\right)}{G(1+t)}.$$

4.4 Further works

Formula (19) can be written

$$\det(I_N - A_N) \overset{\text{law}}{=} X_N \det(I_{N-1} - A_{N-1}),$$

where A_{N-1} (resp A_N) is distributed with the Haar measure $\mu_{U(N-1)}$ (resp $\mu_{U(N)}$), and X_N is a random variable independent of A_{N-1}. Can we directly (ie : without the Selberg integrals) find such a formula ?

A recursive decomposition of the Haar measure, presented in [2] will give a positive answer to this question, not only for the unitary group but also for $O(n)$, $SO(n)$, $USp(2n)$...

Moreover, further developments about the characteristic polynomials of random matrices linked to these notes might be the following :

- Is it possible to extend formula (19) for the characteristic polynomial $\det(I_N - xA)$, and not only for its value at $x = 1$?
- For distinct angles θ_1 and θ_2, what is the asymptotic law of $Z_N(A, \theta_1)Z_N(A, \theta_2)$?

References

[1] G. E. Andrews, R. A. Askey, R. Roy, Special functions, Encyclopedia of Mathematics and its Applications, 71, Cambridge University Press, Cambridge, 1999.

[2] P. Bourgade, C. P. Hughes, A. Nikeghbali, M. Yor, The characteristic polynomial of a unitary matrix : the probabilistic approach, in preparation.

[3] L. Chaumont, M. Yor, Exercices in probability, vol 13 in Cambridge Series in Statistical and Probabilistic Mathematics, Cambridge University Press, Cambridge, 2003.

[4] S. M. Gonek, C. P. Hughes and J. P. Keating, A hybrid Euler-Hadamard product formula for the Riemann zeta function, preprint, 2005.

[5] J. Jacod, personal communication, 2006.

[6] C. P. Hughes, J. P. Keating and N. O'Connell, On the characteristic polynomial of a random unitary matrix, Comm. Math. Phys. 220, n°2, p 429-451, 2001.

[7] C. P. Hughes, A. Nikeghbali, M. Yor, in preparation (April 2006).

[8] J. P. Keating and N. C. Snaith, Random Matrix Theory and $\zeta\left(\frac{1}{2} + it\right)$, Comm. Math. Phys. 214, p 57-89, 2000.

[9] F. Mezzadri, How to generate random matrices from the classical compact groups, preprint, September 2006.

[10] S. J. Patterson, An Introduction to the Theory of the Riemann Zeta-Function, Cambridge Studies in Advanced Mathematics, New Edition, 1995.

[11] M. Yor, Interpretations in terms of Brownian and Bessel meanders of the distribution of a subordinator perpetuity, p 361-375. In : Lévy processes - Theory and Applications, eds : O. Barndorff-Nielsen, T. Mikosch, S. Resnick. Birkhäuser, 2001.